REMARKS

In response to the Office Action dated November 13, 2009, Applicants respectfully requests reconsideration. Claims 1-10, 13-16, 18-23 and 25-45 were previously pending in this application. By this amendment, claims 1, 16, 22 and 40 have been amended. New claims 46 and 47 have been added. Claims 13 and 15 have been canceled without prejudice or disclaimer. As a result, claims 1-10, 14, 16, 18-23 and 25-47 are pending for examination with claims 1, 16, 22 and 40 being independent claims. No new matter has been added.

Rejections Under 35 U.S.C. §103

I. Claims 1 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, U.S. Patent Publication No. 2003/0074359 (Tezuka) in view of Mayer, U.S. Patent Publication No. 2002/0178,246 (Mayer), in further view of Gupta et al., U.S. Patent Publication No. 2005/0149948 (Gupta). Before discussing the claims, Applicants provide a brief overview of some embodiments of the invention to assist the Examiner in appreciating various aspects of the present invention. The Gupta reference is also briefly discussed.

Overview of Some Embodiments

Some embodiments relate to a computer connected to one or more computer networks. The computer may determine the network DNA for each of the computer networks and apply the network DNA to a network DNA policy to determine how to configure the computer for the computer network (paragraph [0043]). For example, a network DNA policy may specify that system security settings be configured depending on a network species type (e.g., enterprise, home, or public network) associated with a computer network's network DNA (paragraph [0070]).

The network DNA may have one or more network DNA components whose values are determined from information collected from the computer network (paragraph [0052]). The network species type mentioned above is an example of a network DNA component (paragraph [0052]). The network species may indicate that the computer network is, for example, an enterprise network, a home network, or a public place network depending on the information collected from the computer network (paragraph [0054]). For example, a computer network that is secure,

managed and provides connectivity to an enterprise resource may be classified as an enterprise network (paragraph [0055]). As another example, an insecure, unmanaged, private network may be classified as a home network (paragraph [0056]). The network species determined for a network may be applied to a network DNA policy to determine how to configure security settings of the computer that control communication over a connection to the computer network (paragraph [0070]).

It should be appreciated that the foregoing discussion of embodiments of the invention is provided merely to assist the Examiner in appreciating various aspects of the present invention. However, not all of the description provided above necessarily applies to each of the independent claims pending in the application. Therefore, the Examiner is requested to not rely upon the foregoing summary in interpreting any of the claims or in determining whether they patentably distinguish over the prior art of record, but rather is requested to rely only upon the language of the claims themselves and the arguments specifically related thereto provided below.

Discussion of Gupta

Unlike the embodiments described above in which information about a network is used to determine how to configure a computer connected to that network, Gupta describes a way of controlling connection managers to avoid conflicts that is not based on the network type. Specifically, Gupta describes a wireless device 103 with an integrated connection manager 112 and a number of third party connection managers 118 that may conflict with one another (¶ 3; FIG. 1). A connection manager that is registered with a device driver 109 may customize the configuration of the device's network interface 106 (¶ 3). The customization performed by a third party connection manager 118 is based on a configuration required by a third party application 121 (¶ 16). Because the connection managers may each have their own unique policies, Gupta prevents the connection managers from concurrently registering with the device driver 109 (¶ 15). Accordingly, the device driver 109 monitors for network access data, that is, attempts to control, configure or access the network interface by one of the connection managers (¶ 12; FIG. 5A, step 503). The connection manager 112 has policies that determine whether a third party connection manager 118 registered with the device driver should be disabled (¶ 42; FIG. 5A, step 515). The policy may

direct the connection manager 112 to unregister a third party connection manager 118 under one set of circumstances and may direct the connection manager 112 to disable the third party connection manager 118 under a second set of circumstances (¶ 38).

Independent Claim 1

As amended, claim 1 recites, *inter alia*:

> initiating on the computer connected to the computer network an execution of a network DNA policy action of the network DNA policy, the execution of the network DNA policy action configuring network security settings of the computer that control communication over a connection to the computer network when the network DNA policy condition of the network DNA policy is satisfied.

This claim distinguishes over the cited references. The Office Action admits on page 5 that Tezuka and Mayer are silent on disclosing this limitation and cites Gupta to meet this limitation. Applicants respectfully disagree. As discussed above, Gupta's policy decisions are not based on network conditions at all. Rather, Gupta describes policies where the connection manager 112 disables (unregisters) a third party connection manager 118 when it simply attempts to access or configure the network interface (¶ 13, 38, 42; FIG. 1). Gupta describes another set of policies which act based on the requirements of a third party application (¶ 3, 16). Clearly none of Gupta's policy decisions are based on network conditions. By contrast, claim 1 recites "initiating... the execution of the network DNA policy action... ***when the network DNA policy condition of the network DNA policy is satisfied***".

Claim 1 distinguishes for other reasons as well. The Office Action asserts on page 6 that "allowing or disallowing the connection based on network policy is equivalent to configuring network security settings executed by the network DNA policy." Disallowing the connection cannot meet this limitation of claim 1 as it specifically recites that "the computer [is] connected to the computer network." Further, claim 1 requires more than merely allowing a connection as the claim specifically recites "***configuring network security settings*** of the computer ***that control communication over a connection to the computer network***."

Accordingly, claim 1 patentably distinguishes over the prior art of record, such that the rejection of claim 1 under 35 U.S.C. §103 should be withdrawn.

Claims 2-10, 13-15 and 45 depend from claim 1, incorporate all of its limitations, and should be allowed for at least the same reasons. Though Applicants do not necessarily concur with the rejections, Applicants believe it is unnecessary to separately address the rejections of the dependent claims. However, the dependent claims also add limitations that further distinguish over the references, and Applicants reserve the right to argue further for the patentability of these claims.

II. Claims 2, 16, 20, 21, 22, 27, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, in view of Mayer, in view of Gupta, in further view of Jemes et al., U.S. Patent Publication No. 2001/0037384.

Independent Claim 16

Applicants respectfully disagree with the Examiner's assertion that Applicants' previous arguments are moot in view of new grounds of rejection. In Applicants' previous response, filed July 6, 2009, Applicants showed that the Tezuka/Mayer/Jemes combination does not disclose "the network species component indicating a network species classification selected from among a plurality of network species classifications, the plurality of network species classifications including an enterprise network, a home network, and a public place network" as recited in claim 16. The Office Action dated April 8, 2009 admitted that Tezuka and Mayer did not disclose this limitation and cited Jemes as purportedly meeting this limitation. The present Office Action admits that Tezuka, Mayer and Gupta do not disclose this limitation and again relies solely on Jemes for meeting this limitation. Accordingly, Applicants respectfully request the Examiner reconsider the arguments for why Jemes does not meet this limitation. For the Examiner's convenience, the arguments from the response filed July 6, 2009 are substantially repeated below.

> Claim 16 clearly distinguishes over the cited references. The Office Action admits that Tezuka and Mayer do not teach "the network species component indicating a network species classification selected from among a plurality of network species classifications, the plurality of network species classifications including an enterprise network, a home network, and a public

place network" as recited in claim 16, but asserts that the feature is taught by Jemes via the Abstract, paragraph 17 and FIG. 2. Applicants respectfully disagree. Jemes describes a secure network system in which network control point devices are configured to enforce a network security policy for the network to which the control point device is connected (Abstract). In paragraph 17, Jemes notes configuring a network security policy in an enterprise network having multiple firewalls creates redundant work and increases the likelihood of error. FIG. 2 shows a secure network system configuration (¶ 22). Jemes describes networks in the secure network system, such as networks 24a, 24b and 24c of FIG. 2, as having either "known" or "unknown" network security policies (¶ 29, 30, 34). By contrast, claim 16 recites "the network species component indicating a network species classification selected from among a plurality of network species classifications, ***the plurality of network species classifications including an enterprise network, a home network, and a public place network.***" Jemes describes networks as having known or unknown security policies, but does not teach or suggest a "plurality of network species classifications including an enterprise network, a home network, and a public place network." In fact, Jemes does not mention a "home network" at all, let alone show a plurality of network species classifications including a home network. The prior art of record simply fails to teach or suggest "determining a network DNA of the computer network, the network DNA comprising the network species component, the network species component indicating a network species classification selected from among a plurality of network species classifications, the plurality of network species classifications including an enterprise network, a home network, and a public place network."

To expedite prosecution, claim 16 has been amended to further recite "the network species component indicating the network species is "enterprise network" if a first network condition is met, the network species component indicating the network species is "home network" if a second network condition is met, and the network species component indicating the network species is "public place network" if a third network condition is met." Support for this amendment is found in the specification, for example, in paragraphs [0055]-[0057]. It should be clear from the above discussion of the references that the Tezuka/Mayer/Gupta/Jemes combination does not meet this limitation of claim 16.

Accordingly, claim 16 patentably distinguishes over the prior art of record, so that the rejection of claim 16 under 35 U.S.C. §103 should be withdrawn.

Claims 18-21 and 46 depend from claim 16, incorporate all of its limits, and should be allowed for at least the same reasons. Though Applicants do not necessarily concur with the rejections, Applicants believe it is unnecessary to separately address the rejections of the dependent claims. However, the dependent claims also add limitations that further distinguish over the references, and Applicants reserve the right to argue further for the patentability of these claims.

Independent Claim 22

As amended, claim 22 recites, *inter alia*:

> and at least one network DNA store configured to store a network DNA for at least one of said at least one computer network, the network DNA taxonomically classifying said at least one of said at least one computer network, and the network DNA comprising at least one derived network DNA component, the at least one derived network DNA component comprising a network species component configured to indicate a network species classification selected from among a plurality of network species classifications, the plurality of network species classifications including an enterprise network, a home network, and a public place network, the network species component indicating the network species is "enterprise network" if a first network condition is met, the network species component indicating the network species is "home network" if a second network condition is met, and the network species component indicating the network species is "public place network" if a third network condition is met.

This claim distinguishes over the cited references. It should be clear from the discussion of the references above in connection with claim 16 that the prior art of record fails to satisfy this limitation.

Accordingly, claim 22 patentably distinguishes over the prior art of record, so that the rejection of claim 22 under 35 U.S.C. §103 should be withdrawn.

Claims 23, 25-39 and 47 depend from claim 22, incorporate all of its limits, and should be allowed for at least the same reasons. Though Applicants do not necessarily concur with the rejections, Applicants believe it is unnecessary to separately address the rejections of the dependent

claims. However, the dependent claims also add limitations that further distinguish over the references, and Applicants reserve the right to argue further for the patentability of these claims.

Independent Claim 40

Claim 40 recites, *inter alia*:

> a network species component configured to indicate a network species classification of the computer network, the network species classification selected from among a plurality of network species classifications including enterprise network, home network and public place network.

This claim distinguishes over the cited references. It should be clear from the discussion of the references above in connection with claim 16 that the prior art of record fails to satisfy this limitation.

As further reason that the references do not meet the limitations of the claim, claim 40 also recites "the network species classification determined as a function of, at least, a type of network security, a type of network management and a type of network addressing." The Office Action states "it is known that computer network comprises of security, network management and addressing attribute." Even if the Examiner's assertion were true, it would not meet this limitation of claim 40. Claim 40 makes clear that the "network species component indicate[s] a network species ***classification of the computer network***." The claim further makes clear that the classification is determined as a function of at least three factors: the type of network security, the type of network management and the type of network addressing. Even if these parameters existed in a network setting, that does not provide a reason that they would have been used as recited by the claim. The claim requires determining the network species classification as a function of, at least, a type of network security, a type of network management and a type of network addressing, which is not shown in any of the references.

Accordingly, claim 40 patentably distinguishes over the prior art of record, so that the rejection of claim 22 under 35 U.S.C. §103 should be withdrawn.

Claims 41-44 depend from claim 40, incorporate all of its limits, and should be allowed for at least the same reasons. Though Applicants do not necessarily concur with the rejections, Applicants believe it is unnecessary to separately address the rejections of the dependent claims.

However, the dependent claims also add limitations that further distinguish over the references, and Applicants reserve the right to argue further for the patentability of these claims.

New Claims 46 and 47

Claims 46 and 47 are added to further define Applicants' contribution to the art. Claims 46 and 47 depend from claims 16 and 22 respectively. The new claims are supported in the specification, for example, in paragraphs [0055]-[0057]. Claims 46 and 47 are allowable based at least on their dependency. The new claims recite additional limitations not met by the references.

Comments on Dependent Claims

Since each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Applicants believe that it is unnecessary at this time to argue the allowability of each of the dependent claims individually. Applicants do not, however, necessarily concur with the interpretation of the dependent claims as set forth in the Office Action, nor do Applicants concur that the basis for the rejection of any of the dependent claims is proper. Therefore, Applicants reserve the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered, please charge any deficiency to Deposit Account No. 23/2825.

Dated: 1-22-10

Respectfully submitted,

By _____

Edmund J. Walsh
Registration No.: 32,950
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
617.646.8000